Document Generated: 11/10/2026

Learning Style: On Demand

Technology: EC-Council

Difficulty: Intermediate

Course Duration: 32 Hours

Computer Hacking Forensic Investigator Certification (CHFI)



What's Included:

- *Official EC Council Training Videos*
- *Official EC Council Courseware included*
- *Official EC Council ilabs included*
- *EC Council Exam Voucher*

The Computer Hacking Forensic Investigator (CHFI) certification provides comprehensive training in digital forensics and computer investigations, equipping professionals with the skills to detect hacking attacks, collect and preserve digital evidence, investigate cybercrimes, and conduct security audits to prevent future incidents. As cybercrime continues to grow worldwide, law enforcement agencies, government organizations, and businesses increasingly rely on computer forensic techniques to investigate offences such as intellectual property theft, trade secret theft, fraud, and data destruction. The CHFI program covers the latest forensic tools, technologies, and methodologies, enabling learners to recover deleted, encrypted, or damaged data, analyse digital evidence, and perform legally sound investigations using industry-recognised computer forensic practices.

Course Objectives:

- Perform incident response and forensics
- Perform electronic evidence collections
- Perform digital forensic acquisitions
- Perform bit-stream Imaging/acquiring of the digital media seized during the process of investigation.
- Examine and analyze text, graphics, multimedia, and digital images
- Conduct thorough examinations of computer hard disk drives, and other electronic data storage media
- Recover information and electronic data from computer hard drives and other data storage devices
- Follow strict data and evidence handling procedures
- Maintain audit trail (i.e., chain of custody) and evidence integrity
- Work on technical examination, analysis and reporting of computer-based evidence
- Prepare and maintain case files

- Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files
- Gather volatile and non-volatile information from Windows, MAC and Linux
- Recover deleted files and partitions in Windows, Mac OS X, and Linux
- Perform keyword searches including using target words or phrases
- Investigate events for evidence of insider threats or attacks
- Support the generation of incident reports and other collateral
- Investigate and analyze all response activities related to cyber incidents
- Plan, coordinate and direct recovery activities and incident analysis tasks
- Examine all available information and supporting evidence or artefacts related to an incident or event
- Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents
- Conduct reverse engineering for known and suspected malware files
- Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event
- Identify data, images and/or activity which may be the target of an internal investigation.
- Establish threat intelligence and key learning points to support pro-active profiling and scenario modelling
- Search file slack space where PC type technologies are employed
- File MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences
- Examine file type and file header information
- Review e-mail communications including web mail and Internet Instant Messaging programs
- Examine the Internet browsing history
- Generate reports which detail the approach, and an audit trail which documents actions taken to support the integrity of the internal investigation

process

- Recover active, system and hidden files with date/time stamp information
- Crack (or attempt to crack) password protected files
- Perform anti-forensics detection
- Maintain awareness and follow laboratory evidence handling, evidence examination, laboratory safety, and laboratory security policy and procedures
- Play a role of first responder by securing and evaluating a cybercrime scene, conducting preliminary interviews, documenting crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting of the crime scene
- Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
- Apply advanced forensic tools and techniques for attack reconstruction
- Perform fundamental forensic activities and form a base for advanced forensics
- Identify and check the possible source/incident origin
- Perform event co-relation
- Extract and analyze logs from various devices such as proxies, firewalls, IPSes, IDSes, Desktops, laptops, servers, SIM tools, routers, switches, AD servers, DHCP servers, Access Control Systems, etc.
- Ensure that reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality
- Assist in the preparation of search and seizure warrants, court orders, and subpoenas
- Provide expert witness testimony in support of forensic examinations conducted by the examiner

Audience:

- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals

- Systems administrators
- Legal professionals
- Banking, Insurance and other professionals
- Government agencies
- IT managers

Prerequisites:

Although not mandatory, the certification is best suited for:

- Security Analysts
- Digital Forensics Investigators
- Incident Response Analysts
- SOC Analysts
- Law Enforcement or Cybercrime Investigators
- IT Professionals looking to specialize in digital forensic

Course Outline:

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Operating System Forensics
- Defeating Anti- forensics Techniques
- Data Acquisition and Duplication
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigating Email Crimes
- Mobile Forensics
- Investigative Reports

Credly Badge:



Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges